資料５

IoT セキュリティ・セーフティ・フレームワーク

～フィジカル空間とサイバー空間のつながりの信頼性の確保～

（案）

目次

1. 本フレームワークの必要性

1-1　CPSF における第 2 層（フィジカル空間とサイバー空間のつながり）

1-1-1　CPSF 概論

サイバー空間とフィジカル空間が高度に融合した産業社会においては、製品・サービスという価値を生み出す工程（サプライチェーン）が従来の定型的・直線的なものから、多様なつながりによる非定型的なものへと変化している。このような新たな価値創造過程（バリュークリエイションプロセス）のセキュリティ上の課題とその対策を整理することによって、新たな産業社会のセキュリティを確保していく考え方をまとめたものが、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）である。CPSF では、「バリュークリエイションプロセスのセキュリティ確保に当たっては、従来のサプライチェーンで想定されているマネジメントの信頼できる企業間のつながりによって付加価値が創造される領域を越えて、フィジカル空間の情報が IoT によってデジタル化され、データとしてサイバー空間に取り込まれ、そうしたデータがサイバー空間で自由に流通することで、多様なデータが新たなデータを生み出して付加価値を創出することや、新たに創出されたデータが IoT によってフィジカル空間にフィードバックされることで新たな製品やサービスを創出するという、新たな付加価値を創造するための一連の新たな活動を視野に入れる必要がある」とし、企業間のつながりに信頼性の基点を置く第 1 層、フィジカル空間とサイバー空間のつながりに信頼性の基点を置く第 2 層、サイバー空間におけるつながりに信頼性の基点を置く第 3 層という異なる 3 つの信頼性の基点を設定し、これらの基点を中心に経済社会全体のセキュリティ上の課題の洗い出しとその対策をまとめている。

1-1-2　第 2 層の位置づけ

第 2 層は、サイバー空間とフィジカル空間の境界であり、その境界において情報が正確に変換されること、つまり転写機能の正確性を確保することを、第 2 層における信頼性の基点としている。一般に、サイバー空間とフィジカル空間の境界は、例えば前記の転写機能を担うセンサやアクチュエータなどから構成される、いわゆる IoT のシステムによって成立している。IoT のようなフィジカル空間とサイバー空間をつなぐ機器・システムは、それを用いるヒトやソシキの企業活動・経済活動に利益をもたらす一方、インシデントが発生した場合には、それを用いるヒトやソシキが損失や責任を負うことになる。したがって、IoT 機器・システムのセキュリティを確保することが、第 2 層におけるセキュリティ対策の中核となる。

一方、第 2 層におけるセキュリティ上の課題は一様ではない。CPSF においても、以下のように複数の事例が示されている。

・　センサの機能に対するサイバー攻撃の結果、フィジカル空間のデータが正しく転写できずに誤ったデータがサイバー空間へ提供され、データを利活用して実施されるオペレーションに対する信頼を喪失

・　サイバー空間からの間違った指示や IoT 機器への攻撃により、フィジカル空間において機器の制御が誤った形で実施され、従業員等への物理的な危害、機器の損壊等による安全上の問題が発生

・　サイバー攻撃等によって IoT 機器・システムの機能が停止

また、サイバー空間とフィジカル空間をつなぐ IoT 機器・システムの管理における課題についても以下のように触れている。

・　組織等において、IoT 機器の担う役割の重要性に応じて、設置区域管理やモニタリングの実施等の多層的な対策の検討が必要。

・　個人によって家庭などに設置される IoT 機器には、組織等による管理が行き届きにくいものが存在するため、盗難、紛失等のリスクを考慮した対策の実施が必要。

このように、第 2 層におけるセキュリティ対策には、IoT 機器・システムに関連する課題の多様性だけでなく、その利用される環境の多様性も踏まえた対応が必要である。こうした多様性に対し、CPSF では、3 層構造アプローチを通じてリスク源と対策要件を整理し、対策要件に対応したセキュリティ対策例を示している。その際には、セーフティの確保を大前提として、機能安全の観点からの対策やサイバーセキュリティ対策を組み合わせて対応することが必要であるとしている。

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に
“転写”する機能の信頼性を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保

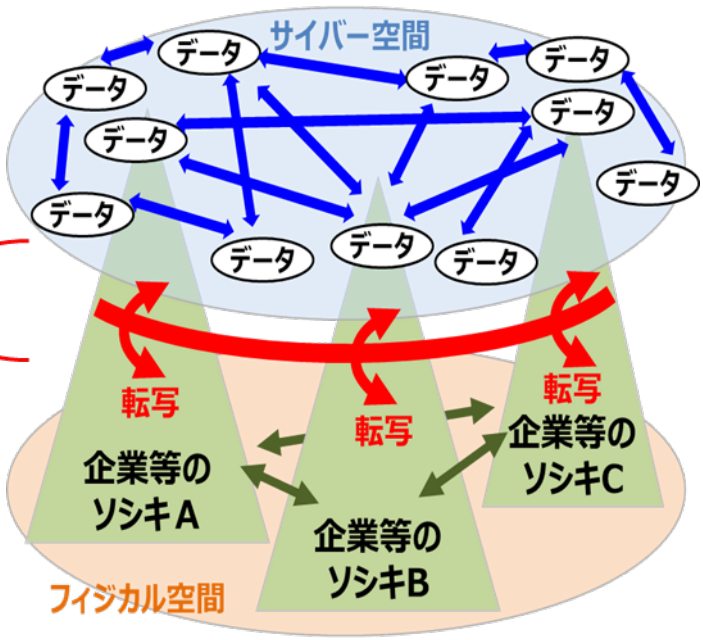

図1 CPSF における 3 層構造モデルと各層における信頼性

1-2 本フレームワークの目的

IoT セキュリティガイドライン[1]でも触れられているように、簡易な情報サービスの分野に使用される IoT 機器と、工場や社会インフラシステム等の安全に関わる分野で使用される IoT 機器では、求められるセキュリティレベル、セキュリティ対策の目的、優先度が異なる。今後、IoT の活用の拡大に伴い、それぞれの分野の特殊性・多様性を踏まえて、使用分野ごとに個別・具体的な IoT 機器・システムに対して実際のセキュリティ対応が進んでいくことになると考えられる。その過程において、サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関して、包括的に課題を捉える統一的な手法が欠如しているため、それぞれの分野/業界において別々の検討プロセスを経て、独自のセキュリティ・セーフティ対策等が設定されることが懸念される。それぞれの対応策に不整合が生じれば、社会として新たな仕組みを受容・管理していくためのコストが増大する恐れがある。

本フレームワークは、上記のような事態を避けるため、サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示するものである。すなわち、異なる分野/業界のプレーヤーがサイバー空間とフィジカル空間をつなぐ機器・システム、つまり IoT 機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための「基本的共通基盤」を提供し、IoT という新たな仕組みを社会として効果的に受容できるようにすることを目的とする。IoT 機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。

なお、本フレームワークでは、サイバー空間とフィジカル空間をつなぐ機器・システムの代表例として IoT、すなわち ”Internet of Things” を捉えているが、本フレームワークはサイバー空間とフィジカル空間をつなぐ機器・システム全般に言えることである。

2. 本フレームワークの想定読者

サイバー空間とフィジカル空間をつなぐ仕組みを構築し、新たな仕組み・サービスを実現していこうとする者は、その仕組み・サービスが様々な形態で実現されることによって、そのセキュリティ上の課題も多様なものにならざるをえないことを認識し、そうした多様性を踏まえた適切なセキュリテ

[1] IoT 推進コンソーシアム、総務省、経済産業省、平成 28 年 7 月策定

ィ対策を講じていかなければならない。新たな仕組み・サービスの革新性が高ければ高いほど、社会で受容していくためには、予想される様々な課題に対応した包括的な対策を講じることが求められることになる。

したがって、本フレームワークは、新たな仕組み・サービスを実現する主体が、新たなリスクに対するセキュリティ対策を講じようとする際に、また、そのような仕組み・サービスを利用する主体が本フレームワークの理解を通じてそのリスクを自ら認識した上でそうした仕組み・サービスを利用する際に、それぞれ参照されることを想定しており、例えば、以下に示すような者を読者として想定している。

- IoT を活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者
- そのような新たな仕組み・サービスで活用される IoT 機器・システムの開発を行う者
- そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする者
- そのような新たな仕組み・サービスを受ける者

3. 本フレームワークの基本構成

3-1 基本構成の背景にある考え方

サイバー空間とフィジカル空間をつなぐ新たな仕組みには様々な形態及びそれに伴うセキュリティ上の課題があり、更に、実際にインシデントが発生した場合の被害の態様も極めて多様である。そのような仕組みを構成する機器・システムに対して一律のセキュリティ要求を設定した場合、仮にその要求が満たされていても、それでは多様なセキュリティ上の課題に十分に対応することはできない。すなわち、利用者等が適切に守られる状況であるとはいえない。

第 2 層のセキュリティ対策を検討する際のポイントは、この多様性に対してどのようにアプローチするのか、ということである。

本フレームワークでは、サイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスの“多様性”という論点にアプローチするための手段として、この仕組みを構成する機器・システム（これ以降「フィジカル・サイバー間をつなげる機器・システム」という。）について、リスクの捉え方とその対応に係る基本的な考え方を集約した 3 つの軸を活用し、カテゴライズするとともに、適切な対策の内容を整理して比較・検討できるようにすることを提案している。

3-2　フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理

フィジカル・サイバー間をつなげる機器・システムのセキュリティ上の課題が実際にインシデントの発生へとつながった場合に影響が出る事象は、人命に関わるようなケースもあれば、プライバシーに関わるケース、資産の毀損に関わるケース、生活環境に関わるケースなど、極めて多様である。つまり、フィジカル・サイバー間をつなげる機器・システムに潜むリスクは多様なものである。

しかしながら、インシデント発生によって影響を受ける事象ごとに整理を行うことは、フィジカル・サイバー間をつなげる機器・システムのセキュリティ対策を検討する上で、その考え方を逆に複雑なものにしてしまうことになる。したがって、影響を受ける事象から何らかの共通項を抽出することによって抽象化した少数の基準に絞り込み、フィジカル・サイバー間をつなげる機器・システムに潜むリスクをシンプルな形で整理できるようにする必要がある。

そのため、本フレームワークでは、様々な人命/身体、プライバシー/名誉、資産、生活環境、経済活動への影響、風評等の影響を受ける様々な事象を以下の 2 つの基準に抽象化して整理し、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいてカテゴライズし、マッピングする 2 つの軸として設定することとした。

3-2-1　第 1 軸：発生したインシデントの影響の回復困難性の度合い

この第 1 軸はインシデントの影響の回復の困難性からリスクを捉えるものである。回復の困難性については、まず、何よりも人命/身体に関する影響から考えることが必要である。言うまでもないが、人命が失われればそれが回復されることはない。また、インシデントの発生の結果、重度の身体障害が発生した場合、完全に回復できるとはいえないケースが少なくない。回復ができるものであったとしても、早期に回復できるケースもあれば、回復に時間を要するケースもある。こうした、インシデントによる影響が回復できるものか否か、また、回復ができるものについては早期の回復ができるか否か、という判断軸を第 1 軸として設定した。

この第 1 軸は、製品安全、労働安全などの分野で法体系によって強制的に要求される安全対策や禁止行為を設定する規制の仕組みの基本的な考え方と同じ立場に立っており、既存の制度体系とも整合性を確保したものである。

第 1 軸では、上記のように、まずは人命/身体の回復不可能な状況を回避するという論点から考え方の整理を進めたが、個人のプライバシー/名誉に関わる情報の中には、一度明らかになってしまえば、本人に回復することができないダメージを与えるような機微な情報も含まれており、こうした本人に回復不可能なダメージを与える情報の保護に関わるような事象も第 1 軸で捉えられる課題に整理されうるものである。

ここで、「リスク」については、インシデントによる影響の度合いと、インシデントの発生確率を用いて捉えることがあるが、本フレームワークでは、フィジカル・サイバー間をつなぐ機器・システムの多様性を踏まえたカテゴライズが容易に行えるように、算出が比較的難しい発生確率は考慮せず、インシデントが発生した場合の影響の度合いからカテゴライズを行うアプローチを採っている。なお、本フレームワークに基づき、産業界での議論等を踏まえた上で具体的な要求を整理する際には、発生確率についても考慮することが適切であることに留意されたい。

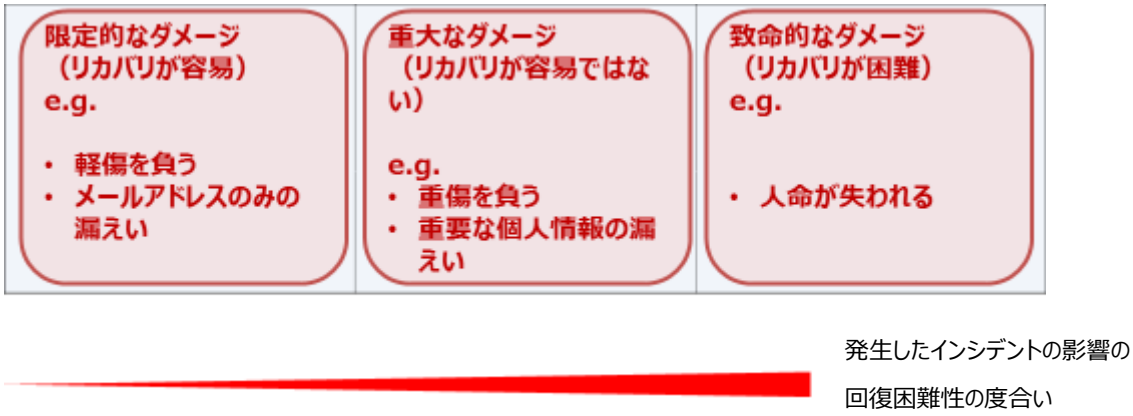

図 2 発生したインシデントの影響の回復困難性の度合いのイメージ

3-2-2 第 2 軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）

第 2 軸は、インシデントによる影響の回復の可能性・困難性という観点を除き、インシデントによる影響の大きさを金銭的価値に換算した場合の大きさ・度合いを基準としたものである。

この基準は、3-2-1 で議論した人命/身体や深刻なプライバシー/名誉に関わるようなケースにおけるインシデントによる影響の回復困難性を考慮したものではなく、その影響の回復については金銭的価値に換算して捉えることが可能なものと仮定し、資産の毀損、経済活動や社会への影響等の事象を第 2 軸に写像して捉えることとした。

第 2 軸は第 1 軸とは独立して考えるべき基準であり、第 1 軸における整理において回復困難性の度合いが低いものとして捉えられたフィジカル・サイバー間をつなぐ機器・システムであっても、第 2 軸では経済的影響の度合いが非常に高いものとして整理されることは十分にある。一方で、第 1 軸における整理において回復困難性の度合いが高いものとして捉えられたフィジカル・サイバー間をつなぐ機器・システムは、実際には賠償金等の形で金銭的価値に換算される中で相応の水準に該当することになる可能性が高い。

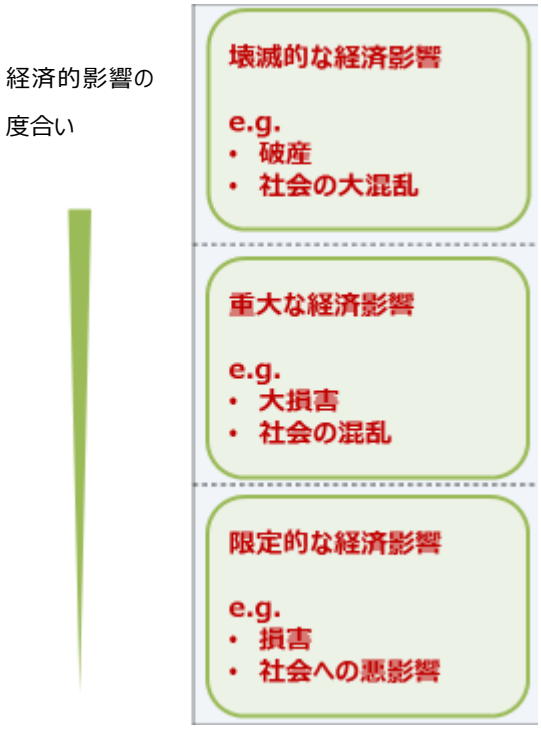

図 3 発生したインシデントの経済的影響の度合いのイメージ

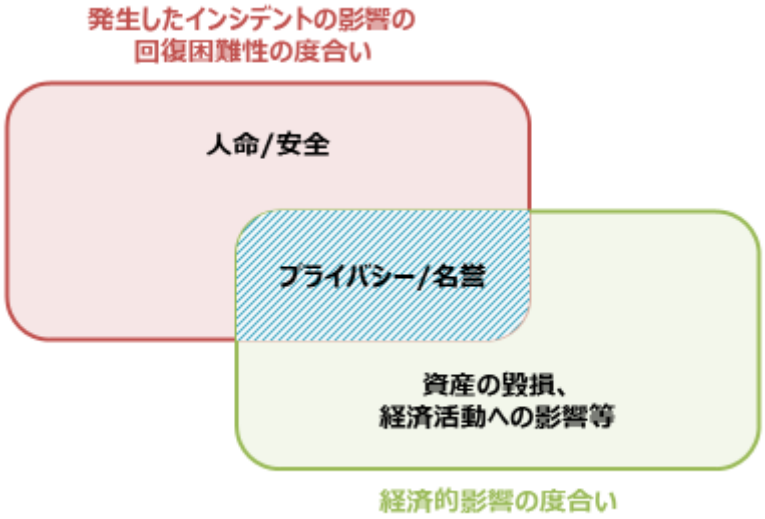

図 4 第 1 軸にも整理されうるプライバシー/名誉の整理

3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ

上述の 2 つの軸に基づいて、フィジカル・サイバー間をつなぐ機器・システムを、当該機器・システムに潜むリスクに基づいてマッピングすることができる。

例えば、第 1 軸では、回復困難性の観点から、限定的なダメージ（回復が容易）、重大なダメージ（回復が容易ではない）、致命的なダメージ（回復が困難）という形で整理し、第 2 軸では、経済的影響の観点から、限定的な経済的影響、重大な経済的影響、壊滅的な経済的影響とい

う形で整理を行うことで、リスクに応じて 9 つの象限（カテゴリ）にカテゴライズすることが可能となる。

それぞれの機器・システムについて適切な対策を検討するに際し、このカテゴリを利用することができる。前述したとおり、フィジカル・サイバー間をつなぐ機器・システムのセキュリティ上の課題は多様であるため、それぞれの機器・システムにおける適切な対策も一様ではない。しかしながら、このカテゴリに基づいて検討を行うことで、一般に右上にカテゴライズされるものほどインシデントによる影響が大きい傾向があるため、より重厚な対策が必要であると考えられる一方、左下にカテゴライズされるものほど、軽微な対策で十分な可能性があると整理することが可能となる。詳細は 3-3 で記載する。

なお、ここでは例として機器・システムのマッピングを行ったが、サービスを構成する機器・システムが提供する機能に着目してマッピングを行うことも考えられる。機器・システムの単位についても、マッピングを行う際に任意に設定できるものである。また、同じ機器であったとしても、どういうシステムで使われるか、システムにおいてどういう役割を持つのか、どのようなスキルを持つ者が使うのか等、その用途により、その重要性や課題、インシデントによる影響等は大きく異なる。そのため、同じ機器でも使用形態などによってマッピング先が異なり得ることに留意する必要がある。

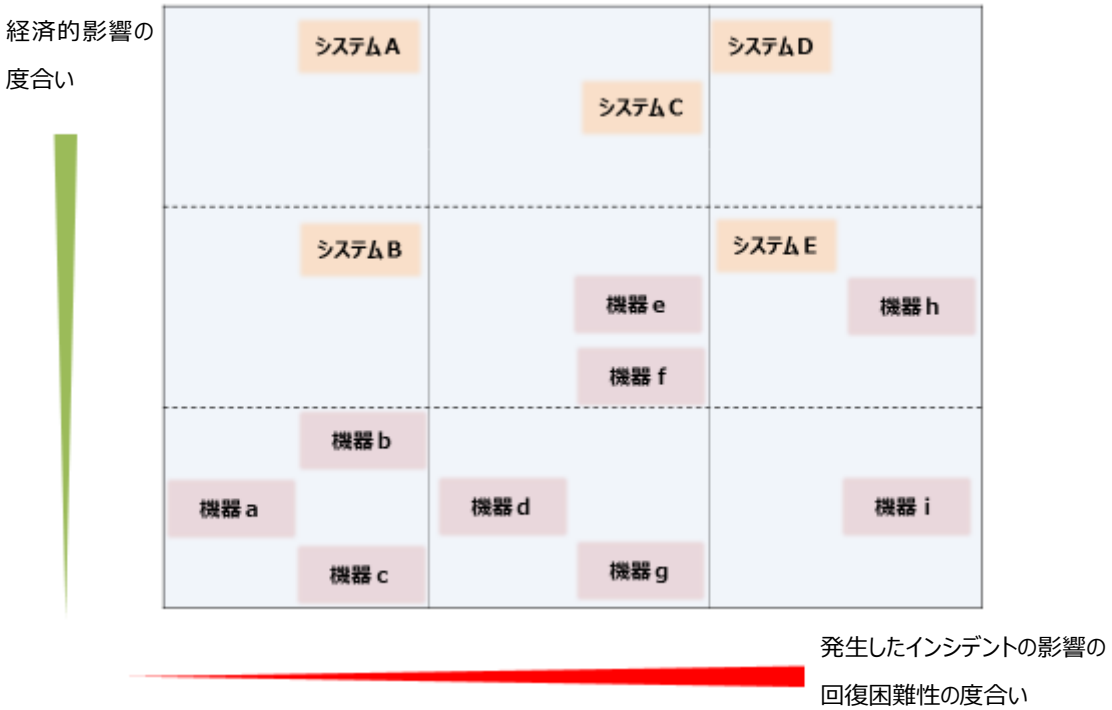

図 5 フィジカル・サイバー間をつなげる機器・システムのカテゴライズのイメージ

（※　同じ機器でも使用形態などによってマッピング先が異なり得る。
例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。）

3-3　求められるセキュリティ・セーフティ要求の整理

上記 3-2-3 のとおり、第 1 軸と第 2 軸を活用し、フィジカル・サイバー間をつなぐ機器・システムについて、そのリスクを踏まえてカテゴライズすることが可能となるが、これだけでは、新たな仕組み・サービスを社会として受容するための具体的な方策を検討することは難しい。そのため本フレームワークでは、フィジカル・サイバー間をつなぐ機器・システムのセキュリティ対策を包括的に整理するために、求められるセキュリティ・セーフティ要求の観点という第 3 軸を設定する。

第 3 軸は、第 1 軸と第 2 軸で形成される平面に直交する形で、いわば 3 次元を構成し、第 1 軸と第 2 軸によって整理されたそれぞれのカテゴリに求められるセキュリティ・セーフティ要求の観点を示す役割を果たすものである。

第 3 軸は、セキュリティ・セーフティを確保するための手法を以下の 4 つの観点から整理している。

図 6　カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ

3-3-1　第 1 の観点：運用前（設計・製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求

フィジカル・サイバー間をつなぐ機器・システムが製造され、実際に利用に供される前の段階で、機器・システムそのものが必要なセキュリティ・セーフティ対策を講じられていること、又は当

該機器等の生産者や供給者、検査者、場合によっては生産設備・工場等が必要な能力条件等を満たしていることなどを確認することを求めるものである。

セキュリティ・セーフティ対策については、その内容を供給者が自ら設定する場合と法令などによって強制的に設定されている場合がある。また、その内容が満たされていることを確認する方法についても、自己適合宣言や第三者による認証など様々な形態があり、求められる確認レベルの専門性や客観性などを踏まえて実際の確認方法が設定されることになる。

3-3-2　第 2 の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求

機器・システムの運用前にセキュリティ・セーフティ対策の実施状況を確認しても、運用中に発生する故障や、実施されるソフトウェアのアップデートやメンテナンスなどによって、想定外の問題が発生する可能性がある。そのような問題が発生していないかを確認するために、運用開始後に、ライフサイクルやサービス期間も考慮しながら機器・システムを確認することを求めるものである。

運用中のセキュリティ・セーフティ対策となるため、より高いレベルのセキュリティ・セーフティを確保することが可能となる。一方で、機器・システムの所有者・運用者が関与するか、機器・システムの所有権・管理権が供給者側に残っているなどの条件が満たされる必要があり、確実な実施を求めていくためには各ステークホルダーにおいて役割や責任分界点を明確化するなど、より社会的な仕組みを用意することが必要となる。なお、ここにおける検査についても、自主検査や第三者による検査など様々な形態を取り得る。

3-3-3　第 3 の観点：機器・システムの運用・管理を行う者の能力に関する確認要求

機器・システムの誤使用・誤操作などによって発生するインシデントの影響が、セキュリティ・セーフティ対策だけでは許容できる水準ではない場合には、機器・システムの運用・管理を行う者が当該機器・システムを適切に運用・管理するために必要な能力を持っていることを確認することを要求することになる。例えば、自動車の場合、運転をする者には一定の技術及び知識を持つことを証明する運転免許の取得を求めており、インシデントが発生した場合の影響が大きいものの、社会的に大きな便益をもたらす技術を社会として受容する社会的な仕組みを構築している。

なお、ここでいう運用者には、サービス提供者のようなシステムを直接操作するわけではないものも含みうる。

3-3-4　第 4 の観点：その他、社会的なサポート等の仕組みの要求

インシデントが発生した場合の影響が非常に大きく、当該仕組み等の所有者が個々に賠償等の対処を実施することが容易ではないケースの場合には、あらかじめ保険加入を義務付けるなどの社会的なセーフティネットを講じることを求めるものである。

例えば、自動車の場合、自動車を所有して運転をする者に対して運転免許の取得を求めることに加え、強制保険である自動車損害賠償責任保険に加入することを義務付けている。これにより、事故を起こした運転者の資力が十分にない場合であっても、被害を受けた者に最低限の賠償が行われるように社会的なセーフティネットを構築している。

なお、第 3 軸における 4 つの観点は、それぞれが必ずしも完全に独立したものではない。例えば、使用者による誤使用や誤操作によるインシデントの発生を回避するためには、第 3 の観点で運用・管理を行う者の能力の確認によって実現するのが適当か、又は第 1 の観点で販売前に使用者に対して使用方法等の情報を提供することを義務化することが適当か、その機器・システムの特徴を踏まえて検討することが必要である。使用方法等の情報を提供する際には、どのようにしてその情報へのアクセシビリティを向上させるかも検討する必要がある。また、必ずしも全ての観点での要求が求められるものではなく、例えば第 2 の観点に係る要求が無くとも、第 1 や第 3 の観点に係る要求により対策を構成することも考え得る。この例のように、複数のステークホルダーが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダーにおける負担について、各ステークホルダーが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて、総合的に検討し、ステークホルダー間で合意する必要がある。したがって、単独のステークホルダーが全ての要求に対処する必要はなく、また、ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である。

さらに、各観点はセキュリティ・セーフティ要求に関する内容の考え方の違いに基づいて設定されたものであり、同じ観点であっても具体的に要求される個々のセキュリティ・セーフティ対策は一様ではない。したがって、仮にセキュリティ・セーフティ要求の観点・内容をコストに換算したとき、第 2 の観点までのセキュリティ・セーフティ要求しか求められていないカテゴリと、第 4 の観点までの全てのセキュリティ・セーフティ要求を求められているカテゴリとコストを比較した場合、前者のコストが必ず低くなるということではないことに留意する必要がある。なお、対策の実施はコストに直結することから、求められるセキュリティ・セーフティ要求に対しどのような対策を取るかは、インシデントの発生確率等も踏まえた上で決定されることが適当である。

各分野において、各観点における具体的なセキュリティ・セーフティ要求事項を詳細に整理することで、本フレームワークをより精緻なものにしていくことが可能である。

4. 本フレームワークの活用方法

サイバー空間とフィジカル空間をつなぐことで生み出される新たな仕組み・サービスは今後様々な形で創出されていくことが予想される。サービスを実現しようとする主体が本フレームワークを活用することにより、フィジカル・サイバー間をつなぐ機器・システムに潜むリスクを踏まえて、機器・システムのカテゴライズを行い、カテゴリ毎に求められるセキュリティ・セーフティ要求の観点を把握し、カテゴリ間で比較することが可能となる。これにより、別々のプロセスで検討した場合であっても、新たな仕組み・サービスに対応したそれぞれの機器・システムに求めるセキュリティ・セーフティ対策の観点・内容の整合性を一定程度確保していくことが可能となる。

その際に注意をしなければならないのは、IoT 機器・システムの用途により、インシデントが発生した場合の影響の内容や大きさが異なるということである。

つまり、本フレームワークは、ある特定の機器に対して一義的にセキュリティ・セーフティ要求の観点を決定するものではなく、実現される仕組み・サービスの利用者側から見てインシデントが発生した場合の影響を適切に分析し、第 1 軸と第 2 軸に従ってカテゴライズを行い、そのカテゴリに従って第 3 軸を活用してセキュリティ・セーフティ要求の観点・内容を適切に検討するための枠組みとなるものである。

本フレームワークを有効に活用していくためには、ユースケースの整理を進めていき、第 1 軸と第 2 軸によるカテゴライズの手法を洗練させていくとともに、ユースケースの蓄積によって第 3 軸によるセキュリティ・セーフティ要求の観点・内容を比較できる環境を整備していくことが求められる。したがって、今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理していくことで、IoT が広く活用されるサイバー空間とフィジカル空間が高度に融合した社会におけるセキュリティ・ セーフティ対策を適切に実施していく制度的対応の整備を進めていくための基礎的条件を整えて行く必要がある。

5. リファレンス

本フレームワークは、サイバー・フィジカル・セキュリティ対策フレームワーク第Ⅰ部、第Ⅱ部で取りまとめた3層構造に基づき、以下の規格等の文書を参照して作成した。

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
IoT セキュリティガイドライン

ISO/IEC 20924
ISO/IEC 27001
IEC 61508 シリーズ
IEC 62443 シリーズ

EN 303 645

EU Cybersecurity Act

SB 327

NIST Cybersecurity Framework
NISTIR 8200, 8228, 8259, 8267, 8276
NIST White Paper: Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

Code of Practice for Consumer IoT Security

ISOC: Internet of Things (IoT) Security Policy Platform Statement